(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
18 January 2001 (18.01.2001)

PCT

(10) International Publication Number
WO 01/05090 A1

(51) International Patent Classification[7]: H04L 9/12, 9/26

(21) International Application Number: PCT/EP00/04627

(22) International Filing Date: 19 May 2000 (19.05.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
1012581 13 July 1999 (13.07.1999) NL

(71) Applicant *(for all designated States except US)*: KONINKLIJKE KPN N.V. [NL/NL]; Stationsplein 7, NL-9726 AE Groningen (NL).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: MULLER, Frank [NL/NL]; Meerkoetlaan 24, NL-2623 NJ Delft (NL). ROELOFSEN, Gerrit [NL/NL]; Rijndijk 60-A, NL-2331 AH Leiden (NL).

(74) Agent: KRUK, Wiggert, Johan; Koninklijke KPN N.V., P.O. Box 95321, NL-2509 CH The Hague (NL).

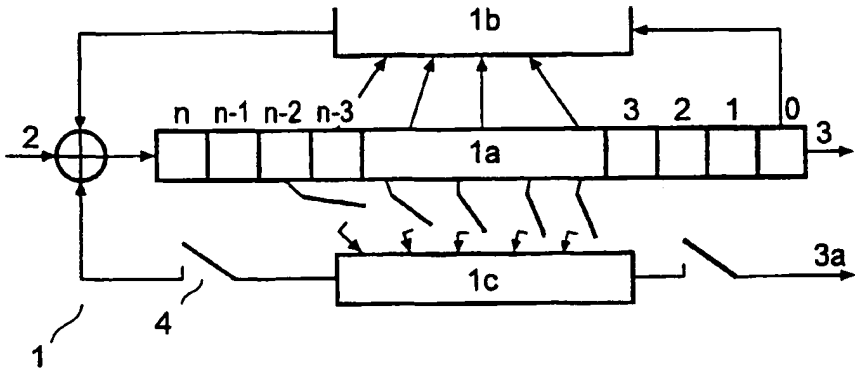
(81) Designated States *(national)*: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *With international search report.*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: A METHOD FOR PROTECTING A PORTABLE CARD



(57) Abstract: A method for protecting a portable card, provided with at least a crypto algorithm for enciphering data and/or authenticating the card, against deriving the secret key used from statistical analysis of its information leaking away to the outside world in the event of cryptographic operations, such as power-consumption data, electromagnetic radiation and the like. The card is provided with at least a shift register having a linear and a non-linear feedback funtion for creating cryptographic algorithms. An algorithm is applied to the card, which is constructed in such a manner that the collection of values of recorded leak-information signals is resistant to deriving the secret key from statistical analysis of said values. Advantageously, after the key has been loaded into the shift register, the shift register clocks on, using at least the linear-feedback function. A suitable alternative is loading only the key into the shift register in the event of a fixed content of the shift register.

WO 01/05090 A1

A method for protecting a portable card.

The invention relates to a method for protecting a portable card, provided with at least a crypto algorithm for enciphering data and/or authenticating the card, against deriving the secret key used from statistical analysis of its information leaking away to the outside world in the event of cryptographic operations, such as power consumption data, electromagnetic radiation and the like, the card being provided with at least a shift register having a linear and a non-linear feedback function for creating cryptographic algorithms, the method comprising loading data to be processed and a secret key in the shift register of the card.

Using a secret key to process input information and/or to produce output information is generally known in the event of cryptographic devices. Using feedback shift registers is also generally known for creating cryptographic algorithms.

In this connection, data to be consecutively processed and a secret key are loaded into one or more shift registers. Here, the sequence of loading data and the key is random.

Subsequently, the output of the shift register and possibly the the shift-register contents are applied, using linear and/or non-linear-feedback, to determine the output of the entire algorithm. The input of the shift register then, apart from the data and the key, also consists of a linear and a non-linear combination of the shift-register contents.

Such shift registers are generally applied in the event of portable cards, such as chip cards, calling cards, smart-card products and the like.

Since the secret key is not known to unauthorised third parties, it is basically impossible to derive either the input or the key from the output of the algorithm.

Now it has become apparent, however, that for chip cards and the like it is possible, in the event of computations, to derive the secret key used from a statistical analysis of the power consumption of the card. Such methods are known as "Differential Power Analysis" (= DPA) and are described in the Internet publication DPA Technical Information: "Introduction to Differential Power Analysis and Related Attacks" by P. Kocher et al., Cryptography Research, San Francisco, 1998.

Said methods are based on the fact that, in practice, with cryptographic operations, information is leaking away to the outside world in the form of power-consumption data, electromagnetic radiation and the like.

Thus, logical microprocessor units show regular transistor-switching patterns which externally (i.e., outside the microprocessor) noticeably produce electrical behaviour.

In this manner, it is possible to identify macro characteristics, such as microprocessor activity, by recording the power consumption and deriving information on the secret key used by way of statistical analysis of the data thus obtained.

The invention now overcomes said drawback and provides a portable card which is resistant to such analyses and therefore provides a card which is safe to use.

The method according to the invention is characterised in that an algorithm is applied to the card which is constructed in such a manner that the collection of values of recorded leak-information signals is resistant to deriving the secret key by way of statistical analysis of said values. Advantageously, after loading the key into the shift register, the shift register is subsequently clocked on, during a specific period of time, several times, at least making use of the linear feedback function.

A suitable alternative according to the invention is loading only the key into the shift register in the event of a fixed content of the shift register.

In a first advantageous embodiment of the invention, there is first loaded the key, subsequently clocking on is performed, after which the data is loaded.

In another advantageous embodiment of the invention, the key is first loaded, subsequently the data is loaded into the shift register, making exclusive use of the linear feedback function and subsequently the clocking on is performed.

In yet another advantageous embodiment of the invention, the data is first loaded, subsequently the key is loaded, making exclusive use of the linear feedback function, whereafter clocking on is performed.

The invention will now be further explained with reference to the drawing and the description by way of non-limiting example.

FIG. 1 schematically shows a typical shift register as applied with a portable card, such as a chip card and the like.

FIG. 2 schematically shows an advantageous solution according to the invention, and

FIG. 3 schematically shows another advantageous solution according to the invention.

Referring now to FIG. 1, there is shown a feedback shift register 1, which is applied in any way suitable for that purpose to a portable card, not shown for simplicity's sake, such as a chip card, calling card and the like, having an input 2 and an output 3.

The feedback shift register 1 comprises a shift register 1a, as well as a feedback function, which in this case consists of a linear function 1b and a non-linear function 1c having an output 3a. Such a feedback shift register, due to its relatively low costs, is eligible for being applied to, e.g., calling cards and the like. The non-linear function may see to it that each bit depends on each number of key bits.

Shift registers are generally known and their operation will therefore not be described in detail. The shift register 1a consists of a series of bits. The length of a shift register is expressed in bits; in the event of a length of n bits, it is called an n-bit shift register.

Each time a bit is required, all bits in the shift register are shifted 1 bit to the right. The new left bit is calculated as a function of the bits remaining in the register and the input.

The output of the shift register is 1 bit, often the least significant bit. The period of a shift register is the length of the output series before repetition starts.

Data is loaded by way of the input 2; the key is loaded, and results are produced by way of the output 3 or, if so desired, 3a. In a similar situation, however, there may be carried out an attack on the secret key used by way of DPA, based on power variations of the system in the event of computations via statistical analysis of "leak data" and error-correcting techniques.

In this connection, it should be noted that, from a security viewpoint, it is desirable to load the key and the data non-linearly into the shift register. It has become apparent, however, that in the event of calculations, non-linearly loading the key and the data into the shift register increases the chance of deriving the secret key used through statistical analysis of the power consumption.

In FIG. 2 and FIG. 3, the same reference numerals as used in FIG. 1 refer to the same components.

FIG. 2 now shows an advantageous embodiment of the invention, the key first being loaded into the shift register, subsequently data being loaded, at least initially, exclusively using the linear-feedback function, and then the clocking on (e.g., 100 times or over) of the shift register taking place. During loading the data and, if so desired, the subsequent clocking on, the non-linear function of the shift register is deactivated until the shift register has been sufficiently clocked on. Then, the non-linear function is switched on once again.

In doing so, the linear-feedback function 1b continues to be active.

Deactivating and activating, as the case may be, the non-linear function 1c may take place in any way suitable for that purpose, e.g., using switches.

The shift register 1a is advantageously clocked on so many times that the content of all elements of the shift register depends on a large portion of the bits of the key.

In another advantageous embodiment, after loading the key there is first clocked on until the content of all elements of the shift register depends on a large portion of the bits of the key. Only after said clocking on, the data in the shift register 1a is permitted to be loaded and non-linear operations on the content of the shift register are also permitted to be effected.

Clocking on takes place in any way known to those skilled in the art and will therefore not be explained in further detail.

For completeness' sake, it should be noted that DPA is only capable of being carried out if there takes place a non-linear operation of the data with the key. Since, in addition, the effort required for DPA rises exponentially with the number of key bits on which the bits in the shift register depend, it is achieved in this manner that, in the event of sufficient interim clocking on of the shift register 1a, applying DPA does not result in short-term success.

In FIG. 3, there is shown an advantageous variant of the invention, the key having been loaded with a fixed content of the shift register (which may also consist purely of zeros) and clocking on the shift register taking place with an active linear and an active non-linear feedback function, but without data being loaded into the shift register during the clocking-on period. In doing so, the input of data into the shift register after loading the key is disconnected from the shift register and is reinstated again after a

specific clocking-on period. Due to the fixed content of the shift register, it is not permitted to apply any modifications and an unauthorised third party shall not be capable of determining a collection of different values of leak data, such as power consumption, and subject it to statistical analysis in order to retrieve the key.

In this solution according to the invention, the key may therefore be loaded non-linearly, and deactivating the non-linear feedback function will not be required.

In another advantageous embodiment of the invention, in the event that the key, after data has been loaded into the shift register, is not loaded with the fixed content of the shift register, the key is loaded into the shift register using only the linear-feedback function, whereafter subsequent clocking on is permitted to take place.

After the aforementioned description, various modifications of the method according to the invention will become apparent to those skilled in the art.

Such modifications shall be deemed to fall within the scope of the invention.

CLAIMS

1. A method for protecting a portable card provided with at least a crypto algorithm for enciphering data and/or authenticating the card against deriving the secret key used from statistical analysis of its information leaking away to the outside world in the event of cryptographic operations, such as power-consumption data, electromagnetic radiation and the like, the card being provided with at least a shift register having a linear and a non-linear feedback function for creating cryptographic algorithms, the method comprising loading data to be processed and a secret key in the shift register of the card, characterised in that an algorithm is applied to the card which is constructed in such a manner that the collection of values of recorded leak-information signals is resistant to deriving the secret key by way of statistical analysis of said values.

2. The method according to claim 1, characterised in that, after the key has been loaded into the shift register, the shift register subsequently, during a specific period, clocks on several times, at least using the linear-feedback function.

3. The method according to claim 2, characterised in that the shift register is clocked on for so long that the content of all elements of the shift register largely depend on the bits of the key.

4. The method according to claim 2 or 3, characterised in that, after the key has been loaded and after clocking on, the data is subsequently loaded into the shift register.

5. The method according to either of the claims 2 and 3, characterised in that after the key has been loaded into the shift register, the data is loaded using only the linear-feedback function and the shift register subsequently clocks on.

6. The method according to any one of claims 2 to 5, characterised in that clocking on the shift register takes place with an active linear-feedback function and a non-active, non-linear feedback function of the shift register.

7. The method according to any one of claims 2 to 6, characterised in that clocking on the shift register takes place with an active linear and an active non-linear feedback function of the shift register, no data being loaded into the shift register, however, during, or prior to, the clocking-on period or prior to loading the key.

8. The method according to any one of claims 5 to 7, characterised in that the non-linear feedback function is deactivated by disconnecting the connections thereof with the shift register as well as, if so desired, with the input.

9. The method according to any one of the claims 4 to 8, characterised in that the input of data into the shift register after loading the key into the shift register is disconnected from the shift register and is reinstated after the aforementioned specific period.

10. The method according to any one of the preceding claims 1 to 9, characterised in that the key is only loaded into the shift register in the event of a fixed content of the shift register.

11. The method according to any one of the preceding claims 1 to 9, characterised in that, if the key is not loaded with a fixed content of the shift register, the key is loaded into the shift register using only the linear-feedback function, whereafter clocking on takes place.

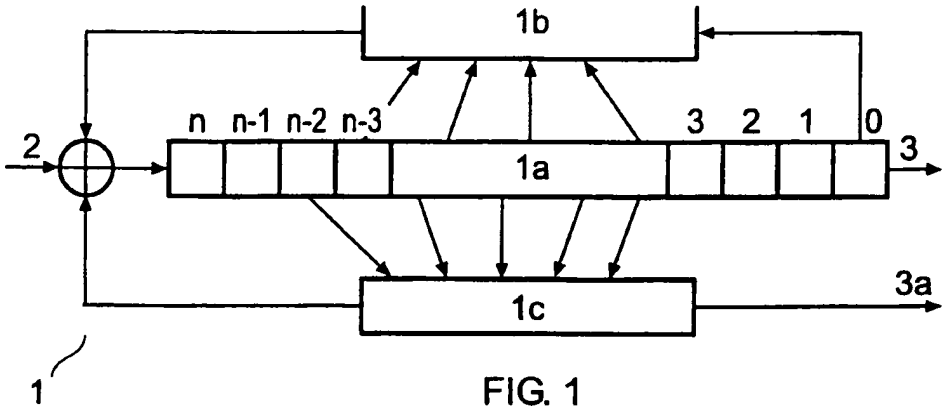


FIG. 1

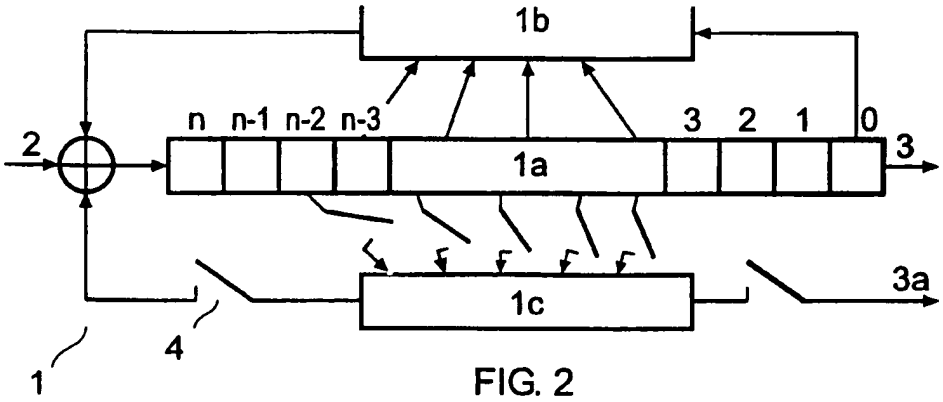


FIG. 2

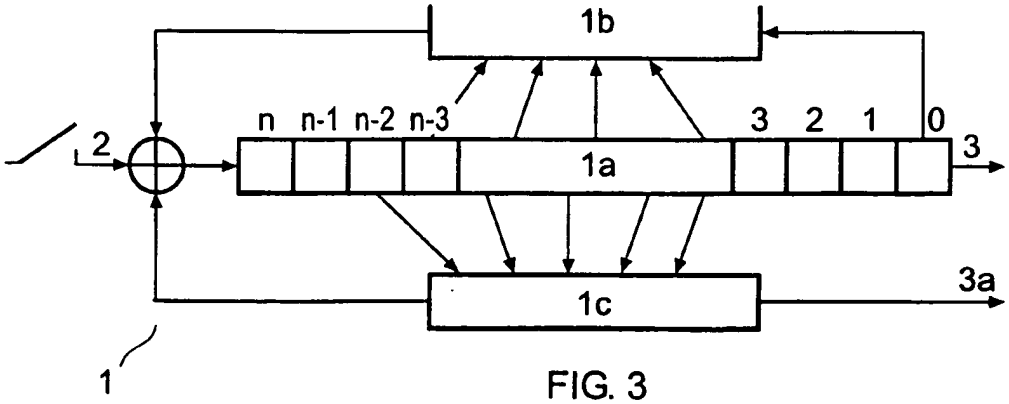


FIG. 3

INTERNATIONAL SEARCH REPORT

Internationa pplication No
PCT/EP 00/04627

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L9/12 H04L9/26

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	DE 196 22 533 A (DEUTSCHE TELEKOM AG) 11 December 1997 (1997-12-11) abstract column 2, line 55 -column 3, line 13 claim 9	1,2,4,6, 7
Y	KOCHER P C: "TIMING ATTACKS ON IMPLEMENTATIONS OF DIFFIE-HELLMAN, RSA, DSS, AND OTHER SYSTEMS" PROCEEDINGS OF THE ANNUAL INTERNATIONAL CRYPTOLOGY CONFERENCE (CRYPTO),DE,BERLIN, SPRINGER, vol. CONF. 16, 1996, pages 104-113, XP000626590 ISBN: 3-540-61512-1 abstract page 112, line 13 - paragraph 3	1,2,4,6, 7

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
31 August 2000	06/09/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Holper, G

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP 00/04627

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5 365 585 A (PUHL LARRY C ET AL) 15 November 1994 (1994-11-15) column 4, line 13 - line 61 ---	1
A	WO 98 52319 A (YEDA RES & DEV ;FLEIT LOIS (US)) 19 November 1998 (1998-11-19) abstract -----	1

1

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP 00/04627

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
DE 19622533 A	11-12-1997	AU 3032197 A	05-01-1998
		CA 2244126 A	11-12-1997
		CN 1221507 A	30-06-1999
		WO 9746983 A	11-12-1997
		EP 0909434 A	21-04-1999
US 5365585 A	15-11-1994	BR 9405567 A	08-09-1999
		CA 2146439 A,C	09-03-1995
		EP 0672273 A	20-09-1995
		FI 951946 A	25-04-1995
		GB 2286274 A,B	09-08-1995
		HK 1002338 A	14-08-1998
		JP 8503569 T	16-04-1996
		KR 168504 B	15-01-1999
		WO 9506906 A	09-03-1995
WO 9852319 A	19-11-1998	US 5991415 A	23-11-1999
		AU 7568598 A	08-12-1998
		EP 0986873 A	22-03-2000